REMARKS

Applicants respectfully request reconsideration of the present application in view of the foregoing amendments and in view of the reasons that follow. Claims 29, 33, 36, 37, 40, 42-44, 46, 48, 54, 60-61, 63, 65, 66, 71, 76, 81, 84, and 87 have been amended. Claims 68, 73, and 78 have been canceled. Applicants respectfully submit that no new matter has been added. Claims 29-67, 69-72, 74-77, and 79-89 are now pending in this application.

I. Rejection of Claims 29-65 Under 35 U.S.C. § 112

On page 3 of the Office Action, Claims 29-65 were rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. On page 3 of the Office Action, the Examiner states:

> The claims recite ' . . . identifying a number of identifications allowed,' further the number of identifications allowed is used to calculate a first address. However, in the specification there is no mention of identifying a number of identification allowed. Furthermore there is no mention of using the value to calculate the first address.

Applicants respectfully submit that Claims 29-65 fully comply with the requirements of 35 U.S.C. § 112, first paragraph, because Applicants' specification describes the claimed subject matter in such a way as to (at least) reasonably convey to one skilled in the art that Applicants, at the time this application was filed, had possession of the claimed invention.

For example, on page 24, lines 5-22, Applicants' specification provides (italics in original, with emphasis added through underlining):

> In another embodiment of the invention described below, in order to prove that the user owns the IP address, the invention describes, in accordance with another implementation, a new way to generate the IP address. This solution is based on using one time password for solving the IPv6 address ownership problem.
>
> This embodiment includes a set-up phase wherein a user *A* (or MN) begins with a secret K. Let h( ) be a one way hash function (e.g. OWF). K could actually be the result of a hash function h( ), or the result of a concatenation of different information (e.g. a secret, the destination IP address, etc.).

> A constant t is fixed (e.g. t=100 or 1000), defining the number of identifications to be allowed. (The system is thereafter restarted with a new K to avoid replay attacks)
>
> *A* computes the suffix (one time password) using K, e.g. using the equation $K_0=h^t(K)$, and generates the IP address IP_A as the concatenation of the prefix (advertised in the router advertisement messages) and K_0 (one time password):
>
> IP_A=Prefix || K_0.

As such, Applicants respectfully submit that Applicants' specification describes the claimed subject matter in such a way as to (at least) reasonably convey to one skilled in the art that Applicants, at the time this application was filed, had possession of the claimed invention. Therefore, Applicants respectfully submit that Claims 29-65 fully comply with the requirements of 35 U.S.C. § 112, first paragraph. Therefore, Applicants respectfully request withdrawal of the rejection of Claims 29-65 under 35 U.S.C. § 112, first paragraph.

II. Rejection of Claims 29-89 Under 35 U.S.C. § 103

A. Rejection of Claims 29-65 Under 35 U.S.C. § 103

On page 3 of the Office Action, Claims 29-65 were rejected under 35 U.S.C. § 103 as being unpatentable over an article titled *Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses* by Montenegro et al. (Montenegro) in view of U.S. Patent No. 5,475,839 to Watson et al. (Watson) in view of U.S. Patent No. 6,971,005 to Henry et al. (Henry). Applicants respectfully disagree. However, to expedite the issuance of this application as a patent, Applicants have amended Claim 29 to further recite "identifying a secret value, wherein the number of identifications allowed is based on a maximum number of times the secret value may be iterated before the secret value is changed." Independent claims 36, 42, 48, 54, and 60 have been similarly amended. The amendment clarifies the number of identifications allowed element of Claims 29-65.

Montenegro, Watson, and Henry, alone and in combination, fail to teach or suggest all of the claim elements, and in particular, fail o teach or suggest "identifying a secret value, wherein the number of identifications allowed is based on a maximum number of times the secret value may be used before the secret value is changed"

On page 2 of the Office Action, the Examiner apparently acknowledges that Montenegro does not disclose or suggest at least "identifying a number of identifications allowed," as recited in Claim 29. In this regard, on page 2 of the Office Action, the Examiner states (with emphasis added through underlining):

> Montenegro teaches the public key as disclosed by the applicant. This public key has a private key pair and therefore the public key is based on the public key and thus it follows that the address of Montenegro is based on the private key pair that is dependent on the public key. Furthermore, the newly cited art teaches the identification allowed.

As such, on page 4 of the Office Action, the Examiner cites Watson as disclosing the noted feature. On page 4 of the Office Action, the Examiner states: "Watson teaches a method of securing access to a computer (title). The system includes identifying a number of identifications allowed (Fig. 5)."

Applicants respectfully submit that the cited portions of Watson do not disclose or suggest the noted features. Fig. 5 of Watson is a flow chart depicting the operation of a system in which a number of unsuccessful login attempts is tracked and compared against a threshold value. Watson discloses:

> Thus, after the initial threshold value (in this example, 3) of unsuccessful login attempts is reached, the system is locked up and must be rebooted, after which only one invalid login attempt is allowed before requiring the system to be rebooted. In one embodiment of this invention, the programmable threshold value is reset to its normal value (in this embodiment, 3) in response to to a valid login.

(Col. 14, lines 25-33, emphasis added through underlining).

Applicants respectfully submit that programming a threshold number of failed login attempts, as disclosed in Watson, is distinguishable from "identifying a number of identifications allowed," as recited in Claim 29.

Moreover, to expedite issuance of this application as a patent, Applicants have amended Claim 29 to further distinguish the claimed subject matter from the cited references. That is, Applicants have amended Claim 29 to further recite: "wherein the number of identifications allowed is based on a maximum number of times the secret value may be used before the secret value is changed." Applicants respectfully submit that Watson does not

disclose or suggest at least this feature. Watson describes resetting of a secret value after a user fails to correctly enter the secret value a certain number of times. Thus, the secret value is not being used when the machine is locked up.

On pages 4-5 of the Office Action, the Examiner cites Henry as disclosing other features of Claim 29. On pages 4-5 of the Office Action, the Examiner states:

> Henry teaches calculating a first address value based on the identified number of identifications allowed; identifying a number of confirmations previously performed between the first device and the second device (column 3 lines 45-50). Since the values can only be calculated after a successful logon and therefore the first address is a value based on the number of times the user is allowed to identify themselves.

Applicants respectfully submit that the cited portion of Henry (i.e., col. 3, lines 45-50) does not disclose or suggest the noted features. For example, in the cited portion, Henry discloses that "an authentication server can be configured to reject any access attempt after several failures" (col. 3, lines 46-47, with emphasis added through underlining). This aspect of the server in Henry appears similar to the system of Watson, as described above.

As such, Applicants respectfully submit that the cited portion of Henry does not disclose or suggest "identifying a number of identifications allowed" or "wherein the number of identifications allowed is based on a maximum number of times the secret value may be used before the secret value is changed," as recited in Claim 29.

As a result, Applicants respectfully submit that Claim 29 is patentable over Montenegro in view of Watson and in view of Henry. Therefore, Applicants respectfully request withdrawal of the rejection of Claim 29 under 35 U.S.C. § 103(a). Claims 30-35 depend from Claim 29. Therefore, Applicants also respectfully request withdrawal of the rejection of Claims 30-35.

At least for reasons similar to those explained with respect to Claim 29, Applicants respectfully submit that independent Claims 36, 42, 48, 54, and 60 are patentable over Montenegro in view of Watson and in view of Henry. Therefore, Applicants respectfully request withdrawal of the rejection of Claims 36, 42, 48, 54, and 60 under 35 U.S.C. § 103(a). Claims 37-41, 43-47, 49-53, 55-59, and 61-65 depend from Claims 36, 42, 48, 54, and 60,

respectively. Therefore, Applicants also respectfully request withdrawal of the rejection of Claims 37-41, 43-47, 49-53, 55-59, and 61-65.

B. Rejection of Claims 66-89 Under 35 U.S.C. § 103

On page 7 of the Office Action, Claims 66, 71, 76, 81, 84-85 and 87-88 were rejected under 35 U.S.C. § 103 as being unpatentable over Montenegro in view of a book titled *Applied Cryptography* by Schneier (Schneier). On page 9 of the Office Action, Claims 67-70, 72-75, 77-80, 82, 83, 86 and 89 were rejected under 35 U.S.C. § 103 as being unpatentable over Montenegro in view of Schneier and further in view of U.S. Patent No. 5,778,069 to Thomlinson et al. (Thomlinson).

Applicants respectfully disagree. However, to expedite the issuance of this application as a patent, Applicants have amended Claim 66 to further recite the elements of now canceled Claim 68. Independent claims 71, 76, 81, 84, and 87 have been similarly amended.

Independent claim 66, as amended, recites in part:

> identifying a plurality of random integers, wherein the plurality of random integers are less than a defined maximum;
>
> identifying a plurality of random bits associated with the plurality of random integers;
>
> calculating a plurality of random values by solving the equation $v_i = (-1)^{b_i} \cdot (s_i^2)^{-1} \bmod n$ for $1<i<k$, where v_i is the plurality of random values, b_i is the identified plurality of random bits, s_i is the identified plurality of random integers, n is the defined maximum value, and k is a security parameter;
>
> calculating a first address value based on the calculated plurality of random values;

On page 10 of the Office Action, the Examiner states:

> In reference to claims 68, 73, 78 Montenegro does not disclose a system wherein calculating the plurality of random values comprises solving the equation $v_i = (-1)^{b_i} \cdot (s_i^2)^{-1} \bmod n$ for $1<i<k$, where v_i is the plurality of random values, b_i is the identified plurality of random bits, s_i is the identified plurality of random integers, n is the defined maximum value, and k is a security parameter.

> Thomlinson discloses a pseudo random number generator wherein calculating the first address value comprises applying a hash function to the calculated plurality of random values (Fig. 3). The hash function performs the function of the equation $v_i = (-1)^{b_i} \cdot (s_i^2)^{-1} \bmod n$.

Thus, the Examiner recognizes that Montenegro fails to disclose a system wherein calculating the plurality of random values comprises solving the equation $v_i = (-1)^{b_i} \cdot (s_i^2)^{-1} \bmod n$. The Examiner, however, states that Thomlinson teaches a hash function that performs the function of the equation $v_i = (-1)^{b_i} \cdot (s_i^2)^{-1} \bmod n$. Applicants respectfully disagree. Relative to Fig. 3, Thomlinson states

> FIG. 3 shows a pseudo random number generator 40 according to a first implementation of this invention. The pseudo random number generator 40 includes a random bit seed creating unit 42 and a stream generator 44. The seed creating unit 42 creates an initializing seed of high entropy that is used by the stream generator 44 to generate pseudo random numbers. The stream generator 44 includes an internal state 46 which maintains the current state of the stream generator. The internal state 46 can be configured as a register (e.g., a physical register, buffer, cache, or reserved memory location) which stores bits representative of the current state value.
>
> The seed is input to the internal state register 46 to initialize the stream generator 44. The bit value held in the state register 46 is output to a transformer 48 which generates an output bit string of random bits according to a selected mathematical transformation (e.g., stream ciphers). The transformer 48 also feeds back one or more bits to the state register to alter the bits held therein from a previous bit value to a next bit value. In this manner, the seed is the initial state value in the stream generator 44 from which generation of random numbers is rooted. Following this initialization, the stream generator 44 updates the state value using feed back from the transformer 48 to produce a next bit value for subsequent number generation.
>
> The seed creating unit 42 has an input device 50 which assembles multiple classes of bits from multiple sources into an input bit string. One class of bits gathered by the input device 50 is an internal class of bits which are derived from at least one source internal to the random number generator 40. As an example, the internal class of bits is a static class of bits kept in the generator. The static class of bits is represented by block 52.

(Col. 4, lines 26-58). However, nowhere does Thomlinson describe a hash function based on the equation $v_i = (-1)^{b_i} \cdot (s_i^2)^{-1} \bmod n$.

Schneier discloses cryptographically secure pseudo-random sequences. (*See* pages 44-45, section 2.8). However, Applicants are unable to find in Schneier disclosure or suggest of the equation $v_i = (-1)^{b_i} \cdot (s_i^2)^{-1} \bmod n$.

As a result, Applicants respectfully submit that Claim 66 is patentable over Montenegro in view of Schneier and further in view of Thomlinson. Therefore, Applicants respectfully request withdrawal of the rejection of Claim 66 under 35 U.S.C. § 103(a). Claims 67, 69, and 70 depend from Claim 66. Therefore, Applicants also respectfully request withdrawal of the rejection of Claims 67, 69, and 70.

At least for the reasons explained above with respect to amended Claim 66, Applicants respectfully submit that independent Claims 71, 76, 81, 84, and 87 are patentable over Montenegro in view of Schneier and further in view of Thomlinson. Therefore, Applicants respectfully request withdrawal of the rejection of Claims 71, 76, 81, 84, and 87 under 35 U.S.C. § 103(a).

Claims 72, 74, 75, 77, 79, 80, 82-83, and 85-86 depend from one of Claims 71, 76, 81, and 84. Therefore, Applicants also respectfully request withdrawal of the rejection of Claims 72, 74, 75, 77, 79, 80, 82-83, and 85-86.

Applicants believe that the present application is in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check or credit card payment form being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicants hereby petition for

such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date February 1, 2008

By _____

Callie M. Bell
Attorney for Applicants
Registration No. 54,989

FOLEY & LARDNER LLP
Customer Number: 23524
Telephone: (608) 258-4263
Facsimile: (608) 258-4258